УДК 004.056
Д. Стьопа, О. Ярема
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ VPN

UDC 004.056
D. Stiopa, O. Yarema

METHODS OF SECURING INFORMATION, TELECOMMUNICATION SYSTEMS AND NETWORKS FROM UNAUTHORIZED ACCESS USING VPN TECHNOLOGY

З переходом працівників більшості компаній на віддалений режим роботи (карантинні обмеження через COVID), з'являється потреба безпечного з'єднання та використання ними інтернету або внутрішніх порталів компанії. Тут VPN є як найбільш доречний та зручний у застосуванні.

VPN (Virtual Private Network) вперше розроблений Microsoft в 1996 році, як спосіб об'єднання в мережу робітників, що працюють дистанційно, та безпечно отримувати доступ до внутрішніх ресурсів компанії. Це по суті формує його першочергову цінність, а саме як інструмент для дистанційного режиму роботи, до якого ми звикаємо.

Користь VPN обмежується не лише працівниками та внутрішніми ресурсами компанії. Надзвичайно важливою проблемою в інтернеті є анонімність. Ніхто не хоче, щоб його змогли відслідкувати до його домашньої IP адреси, а так як запити до ресурсів по суті взагалі не анонімні, то зробити це легко. Віртуальні мережі виступають посередником між користувачем і бажаним ресурсом, виключаючи можливість знайти адресу початкового запиту.

VPN використовує методи шифрування каналу та приховання IP адреси, виступаючи в процесі посередником між користувачем та інформацією, що надає безпечний спосіб запиту до ресурсів. Також сервіс може забезпечувати відсутність логування інформації стосовно користувача.

На рисунку 1 зображена абстрактна модель роботи технології VPN, яка умовно позначена як «тунель» який будується між користувачем та ресурсом, до якого надсилається запит. Тунель є зашифрований та не дає можливості небажаному спостерігачу дізнатись про факт запиту.

Рисунок 1. Абстрактне схема роботи VPN

З кількістю віддалених працівників, яка прогресивно і стрімко збільшується, є абсолютно необхідним мати безпечний вихід до ресурсів. Мережі та системи, як домашні так і корпоративні, потребують безпечної та приватної передачі інформації, при якій ззовні ніхто не зможе ні модифікувати ні переглянути запит користувача чи системи.